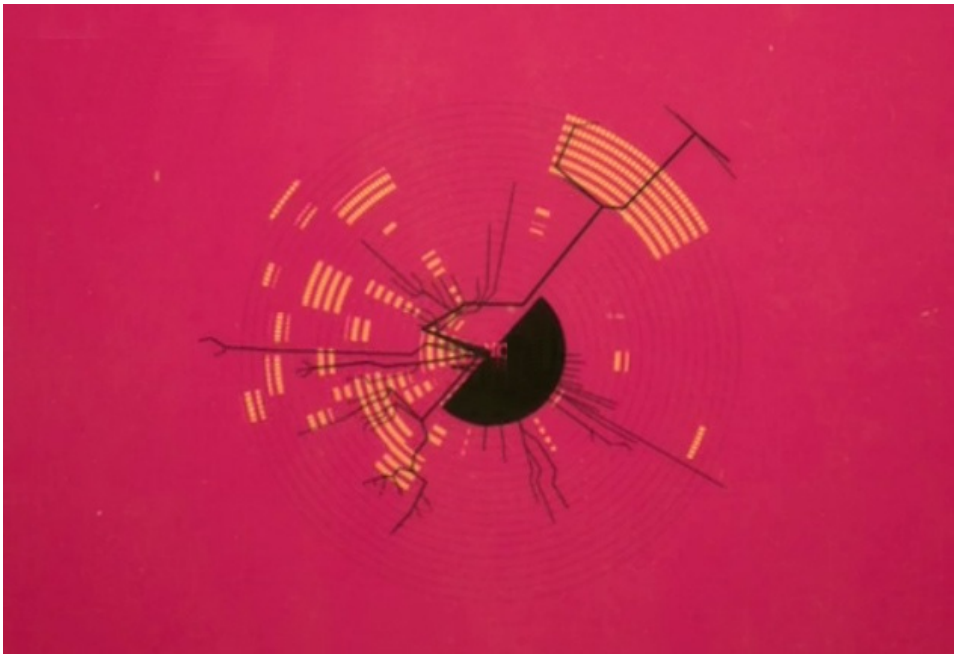
LE MARKETING DÉCLARE SA FLAME

LE 4 JUIN 2012 ***ADRIEN GÉVAUDAN***

Les éditeurs d'antivirus ont récemment révélé l'existence de Flame, logiciel malveillant particulièrement complexe et retors selon les vendeurs de sécurité. A y regarder de plus près, Flame n'est pas si innovant, mais témoigne d'une volonté toujours plus grande des États d'investir le cyberespace. Analyse d'Adrien Gévaudan, du site Intelligence-strategique.eu.



Complexité jugée sans pareille, nom flamboyant, attaques ciblées contre certains intérêts gouvernementaux, Flame a tout d'une cyberarme nouvelle génération. Mais à y regarder de plus près, Flame pourrait ne pas être aussi révolutionnaire que certains médias et entreprises voudraient bien le laisser entendre.

L'alerte a été donnée par Kaspersky, un éditeur d'antivirus à la réputation extrêmement solide. Flame serait le logiciel malveillant le plus complexe découvert à ce jour. **L'éditeur affirme** :

> ***Sa taille est importante, et il est incroyablement sophistiqué. Il redéfinit jusqu'à la notion même de cyberguerre et de cyberespionnage.***

Ses caractéristiques si exceptionnelles… ne le sont cependant pas tant que ça. Flame est un cheval de Troie, à savoir un logiciel permettant à un attaquant de contrôler un système à l'insu de son utilisateur légitime via l'exécution d'un code malveillant. Quelles sont les fonctionnalités de Flame, selon Kaspersky ? Tout de ce qu'il y a de plus commun pour un malware que l'on trouve habituellement dans les milieux cybercriminels.

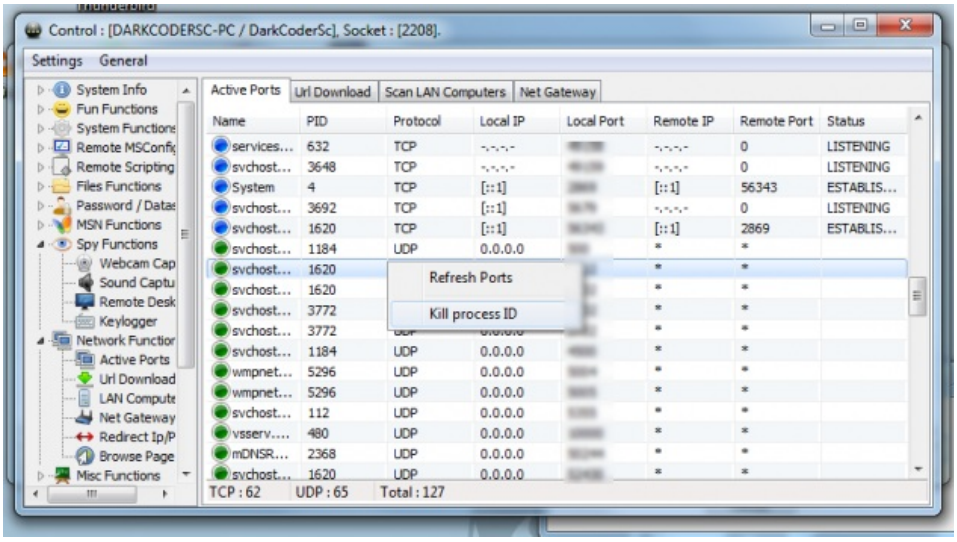
A savoir : la lecture, écriture et suppression de données ; l'exécution de binaires ; la possibilité de prendre des captures d'écran ; l'enregistrement des frappes de clavier (keylogging) et la récupération et l'envoi de fichiers. D'autres fonctionnalités sont un peu plus recherchées telles que l'enregistrement de données audio (si microphone présent) ou la possibilité d'utiliser le

bluetooth et le trafic réseau pour récupérer certaines informations sur l'environnement dans lequel est présent l'ordinateur infecté.

Des fonctionnalités, surprenantes et inquiétantes pour un utilisateur lambda, en réalité extrêmement répandues depuis plus d'une dizaine d'années. A titre d'exemple, le troyen Poison Ivy, dont la première version date de 2005 et qui est toujours librement accessible sur Internet, offre la plupart des fonctionnalités de Flame, décrites par Kaspersky comme constitutives de son originalité ; et bien d'autres encore.

DISSECTION D'UNE NOUVELLE CYBERARME

En 2010, la découverte de Stuxnet changeait la donne en matière de cyberarme. Son perfectionnement dépassait les attentes. ...



A nos yeux, la seule originalité de Flame, outre l'utilisation du **Lua** [Un langage de script, NDLR] restreinte à une micro partie du corps du programme, concerne sa capacité à utiliser le Bluetooth, bien qu'il ne soit fait mention nulle part de la possibilité de se répandre via ce protocole. Même ce qui est présenté par Kaspersky comme la grande spécificité de Flame, à savoir son fonctionnement en modules, n'est pas novatrice.

De très vieux troyens comme MiniMo, NuclearRAT, et bien sûr Poison Ivy fonctionnaient déjà à partir d'un module principal d'infection auquel il était possible, une fois l'accès au système effectif, d'ajouter différents plug-ins selon l'utilisation que l'attaquant souhaitait faire de celui-ci (scanner distant, attaques DDoS, enregistrement de webcam, keylogging, etc.)… Flame, un pétard mouillé ?

Dans **un article publié sur le site *Atlantico***, l'expert en sécurité informatique **Eric Filiol** dénonce le comportement de Kaspersky, et des éditeurs d'antivirus en général, coupables à ses yeux de grossir certaines menaces dans le seul but de faire gonfler leur chiffre d'affaires.

En soi, cette thèse est recevable, et d'autant plus d'actualité que les antivirus ont la très mauvaise habitude de ne pas mettre à disposition les sources de leurs analyses. Cependant, trop occupé à éviter d'avaler la couleuvre de ce très bel exemple d'utilisation marketing de la peur, M. Filiol tombe dans l'excès inverse, celui de la sous-estimation d'une menace peut-être réelle. Les fonctionnalités de Flame que présente Kaspersky ne sont pas nouvelles, et l'éditeur d'antivirus instrumentalise manifestement à son profit la faible connaissance qu'a l'utilisateur lambda de ce qui le menace sur Internet.

Vieilles recettes

Que les fonctionnalités supposées de Flame **soient classiques** ne remet pas en question leur efficacité ; les États utilisent des espions depuis la nuit des temps. Ce même schéma se retrouve dans le domaine du cyber-espionnage, des recettes identiques sont utilisées depuis des années (emails piégés, récole d'information, pivot etc.) sans qu'il y ait de véritable révolution. La société de sécurité RSA **avait été piratée en 2011** à l'aide de Poison Ivy, un RAT disponible sur Internet depuis plus d'une demi-décennie.

Par ailleurs, nombreux ont été les experts informatiques à se gausser de la menace Flame en raison de sa taille importante (environ 20 Mo, tous plug-ins compris) ; même les plus vieux troyens généraient des modules d'infection de quelques centaines de kilo-octets maximum, certains se contentant même avoisiner quelques Ko. Les développeurs de Flame seraient-il donc des "amateurs" ?

Pas nécessairement. Tout d'abord, car rien n'est dit de la possibilité – très probable – que

Flame dispose, si ce n'est à la base, au moins d'un module rootkit. Les rootkits ont la particularité de pouvoir cacher à peu près tout ce qui se trouve sur un système, des fichiers/dossiers aux processus, clés de registre et même le trafic passant par certains ports, qui pourrait indiquer à un observateur avisé que l'ordinateur se comporte d'une façon étrange. Or, si Flame est si complexe, et si, comme Kaspersky en fait mention, il a été capable d'infecter des systèmes Windows 7 entièrement patchés, il est très probable qu'il embarque des fonctionnalités de type Rootkit ou d'élévation de privilèges non-connues publiquement. De plus, comme le dit très justement Félix Aimé, expert en sécurité de l'information [Également auteur sur Intel Strat, NDLR] :

> ***Qui donc vérifie la taille des fichiers sur son disque dur pour en déduire la présence de virus ? La taille d'un virus n'a jamais été un indice de poids dans sa détection, c'est un mythe.***

Enfin, le dernier argument des experts sceptiques sur le cas Flame concerne la soi-disante violation d'un principe de base : *"un code, une cible"* . Bien évidemment, la réussite d'une attaque dépend de sa planification et des informations qu'il a été possible de recueillir sur le système-cible. Mais il est faux de penser qu'un attaquant va coder de A à Z un programme unique, exclusivement adapté à une cible. S'il est vrai qu'un code malveillant se doit d'être adapté aux spécificités du système qu'il vise, un attaquant se contente généralement de moduler un code déjà existant.

Coder à usage unique n'est pas une pratique réaliste et encore moins financièrement viable. En fait, la structure en modules de Flame serait plutôt un argument appuyant sa dangerosité ; peut-être même certains modules ont-ils été codés, à la base, pour une cible en particulier, et ont-ils été au fur et à mesure intégrés au fonctionnement global du malware.

[VIDÉO] STUXNET EN TROIS MINUTES CHRONO

Qui a tout compris à Stuxnet? Pour ceux qui ont encore besoin d'explications, une petite vidéo en motion design devrait ...

Flame ne rédéfinit pas la notion de cyberguerre, comme cela avait été pompeusement annoncé. La menace, en admettant qu'elle soit réelle, n'en est pas pour autant dangereuse pour l'internaute lambda ; il est ici question d'un cheval de Troie, à la diffusion localisée, et qui ne cible que des systèmes appartenant à des personnalités stratégiques. Cependant, la multiplication de malwares si complexes qu'ils peuvent être considérés comme de véritables cyberarmes confirme bien que les États investissent de plus en plus le cyberespace. Et prennent la mesure de son importance stratégique.

Article initialement publié sur **Intelligence-Strategique.eu** sous le titre : ***"Stuxnet, Duqu, et maintenant Flame : course aux cyberarmes ou coup marketing ?"***
Capture d'écran video Stuxnet

MICROSOFT
le 4 juin 2012 - 19:56 • SIGNALER UN ABUS - PERMALINK

Pas un mot sur Microsoft.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

C&C
le 4 juin 2012 - 19:57 • SIGNALER UN ABUS - PERMALINK

Pas un mot sur les infrastructures complexes des C&C.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

F.
le 4 juin 2012 - 21:23 • SIGNALER UN ABUS - PERMALINK

Tu veux savoir quoi sur les C&C ? :)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MSA-2718704
le 4 juin 2012 - 20:42 • SIGNALER UN ABUS - PERMALINK

Microsoft is aware of active attacks using unauthorized digital certificates derived from a Microsoft Certificate Authority.
An unauthorized certificate could be used to spoof content, perform phishing attacks, or perform MITM attacks.

http://technet.microsoft.com/en-us/security/advisory/2718704

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ADRIENGEVAUDAN
le 4 juin 2012 - 20:43 • SIGNALER UN ABUS - PERMALINK

OMG, MY BRAIN o_O

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ADRIENGEVAUDAN
le 5 juin 2012 - 2:04 • SIGNALER UN ABUS - PERMALINK

Super intéressant ce commentaire ; surtout (juste) pour piquer mon nom..!

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GUILLAUME
le 5 juin 2012 - 9:17 • SIGNALER UN ABUS - PERMALINK

A mon humble avis, Flame est juste la manifestation que la technique du hacking est passé de l'ère artisanale à l'ère industrielle. D'où la perte de la notion "une source, un code". Les passionnés feraient bien de s'intéresser aux powerpoints révélés par les spyfiles (Finfisher, Hacking Team notamment).
Flame est un produit à vocation commerciale : il en a la taille (inflation de fonctionnalités sous la pression du marketing), le fonctionnement (un code unique pour plusieurs cibles), la finalité (ce n'est pas un virus, juste un mouchard). C'est le premier (le premier découvert en tout cas) d'une nouvelle génération de produits, à l'usage des gouvernements (ou pas ! C'est bien ça le plus inquiétant : en l'absence de contrôle, toute organisation capable de dépenser quelques dizaines de kEUR par cible peut l'utiliser) pour contourner le "mur du chiffrement".
Peut-être va-t-on bientôt découvrir que pour envoyer les données pompées, Flame utilisait un réseau sophistiqué de serveurs-relais loués par la société qui le commercialise. Qui sait ???
La seule question que Flame pose est la suivante : quand se décidera-t-on à poser les principes de la non-prolifération des armes de cyberguerre ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MARTIN QUINSON
le 6 juin 2012 - 1:55 • SIGNALER UN ABUS - PERMALINK

Je comprend pas la critique disant que flame ne respecte pas la règle “une cible, un code”. Au contraire, même. Une caractéristique qui m’a étonné c’est qu’il ne cherche pas du tout à se propager à tout va : la capacité à se propager par USB est désactivée dès qu’il a réussi à attaquer une machine. C’est peut-être une autre façon de rester indétecté : cibler uniquement les bonnes machines.

Bon, mais sinon la fascination pour les armes, c’est un peu glauque, même quand elles sont cyber. J’ai un peu honte, là :)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

AGEVAUDAN
le 7 juin 2012 - 4:39 • SIGNALER UN ABUS - PERMALINK

Je ne peux qu’être d’accord ; je pense que cette espèce de règle de base arbitrairement définie (d’ailleurs elles sont énoncées où ces règles de base? Par qui?) “une cible = un code” est simplificatrice au possible, en ce qu’elle postule que tout le code d’un malware doit être adapté à une cible.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

KABE
le 6 juin 2012 - 14:11 • SIGNALER UN ABUS - PERMALINK

Vous parlez de ces services qui sont courant pour en déduire que ce malware est finalement banale. Mais la complexité d’un malware n’est pas limité à ces services bien au contraire. Le fait de rendre la rétro-ingénierie difficile, le fait de passer inaperçu face au anti virus ou d’évoluer très facilement pour se recamoufler, le fait de rester anonyme au niveau de l’attaquant même après découverte du malware, le fait de passer de nombreuse sécurité sans réel problème, etc ..
Pour le poids du malware il a été indiqué que c’est principalement 2 module incluant une machine virtuelle pour lua et un autre incluant sqlLite qui prend la majorité de la place, ces modules sont facultatif. Malgré ca il est resté assez longtemps invisible et surtout que grâce à sa capacité de désinstallation on ne sait pas vraiment le degré des infections qui a eu lieu.
Bref je crois qu’il va falloir attendre pour voir ce qu’il avait dans le vendre avant de dire qu’il est banal, je suis pas certain non plus qu’il y ait beaucoup de malware étant signé Microsoft.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE